IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. ANTON PERAIRE-BUENO, and JAMES PERAIRE-BUENO, Defendants.	Case No.: 1:24-cr-00293-JGLC

DEFENDANTS' MEMORANDUM OF LAW
IN SUPPORT OF JOINT MOTIONS TO DISMISS THE INDICTMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES AND RULE

OTHER AUTHORITIES

Defendants Anton Peraire-Bueno and James Peraire-Bueno respectfully submit this memorandum of law in support of their three motions to dismiss the Indictment: (1) Motion to Dismiss the Indictment for Failure to Provide Fair Notice; (2) Motion to Dismiss the Indictment for Failure to Allege Essential Elements; and (3) Motion to Dismiss the Indictment as Unconstitutionally Vague.

INTRODUCTION

This case is novel. The Indictment purports to charge the Peraire-Buenos with one count of conspiracy to commit wire fraud (18 U.S.C. § 1349), one count of wire fraud (18 U.S.C. § 1343), and one count of conspiracy to commit money laundering (18 U.S.C. § 1956(a)(1)(B)(i)), all relating to a series of transactions allegedly executed on the Ethereum cryptocurrency blockchain in April 2023. Its allegations are far removed from the heartland of wire fraud. Describing the alleged fraudulent scheme as "the very first of its kind," Indict. ¶ 1, the Indictment is an audacious attempt by the United States government to regulate, for the first time and through criminal prosecution, the duties and interactions of users of the Ethereum Network—a decentralized, trustless system that uses economic incentives to drive behavior and relies on consensus to effect changes. The Indictment's allegations—and its missing allegations—betray the problems with the government's approach.

The hallmarks of a fraud case are conspicuously absent. The Indictment does not allege that, in executing this alleged scheme, the Peraire-Buenos made a single false or misleading statement, or an omission with a duty to disclose. According to the Indictment, the alleged victims traded away their supposedly lost cryptocurrencies to other users (*i.e.*, not the Peraire-Buenos) through pre-programmed trades without ever interacting with the Peraire-Buenos, directly or indirectly. The Indictment identifies these alleged victims as automated computer programs (or

"bots") that manipulate cryptocurrency markets through speculative trades and seek to profit at the expense of less sophisticated users.

In this novel context, the Indictment alleges that the Peraire-Buenos committed wire fraud by "exploit[ing]" a supposed "vulnerability" in the code of an open-source computer program, the MEV-Boost program, that operates as an optional add-on to the Ethereum Network. The Indictment contends that this alleged code exploitation deprived the alleged victims of their expected profits from their speculative trades. The underlying premise of this wire fraud theory appears to be that the Peraire-Buenos acted contrary to other users' implied expectations in a rapidly evolving trading environment where adversarial trading strategies are executed through automated code without the counterparties even interacting.

This "first of its kind" case is grievously flawed, for several reasons that are evident from the face of the Indictment.

First, stretching the wire fraud statute to reach the facts as alleged in the Indictment offends the Due Process Clause's fair notice requirement. Before this Indictment, no Ethereum user would have understood that thwarting a predatory attempt by "bots" engaged in market manipulation could lead to criminal charges. No court has ever applied these statutes to similar transactions, and the Peraire-Buenos had no reason to know that their alleged conduct may be considered unlawful. Indeed, this case appears to be the first and only federal prosecution alleging the commission of wire fraud by supposedly failing to follow rapidly evolving processes for how new cryptocurrency transactions are added to existing blockchains.

Second, the Indictment fails sufficiently to allege the essential elements of wire fraud. While this case arises in novel circumstances, the criminal statutes at issue are not novel. They have well established elements that the Indictment fails to allege. Wire fraud requires a material

misrepresentation or omission by which a defendant intentionally obtains (or attempts to obtain) the money or property of another. The Indictment alleges no such thing. Although it appends conclusory terms like "false" to the computer-programming steps in its narrative, the Indictment does not allege a single false or misleading representation or omission that altered (or could have altered) the alleged victims' bots' pre-programmed trades. And it was the alleged victims' bots' own trades, not the Peraire-Buenos' alleged trades, that caused their losses.

Third, even if the Indictment barely made out the essential elements of wire fraud, it lacks the necessary factual specificity to pass constitutional muster. The Indictment's superficial allegations fail to adequately articulate the prosecution's theories about how the Peraire-Buenos' actions were false or fraudulent and what property rights were wronged. Left in the dark as to the government's theories, the Peraire-Buenos are unable adequately to prepare for trial.

For each of these reasons, as elaborated below, the Indictment should be dismissed.

BACKGROUND[1]

A. The Alleged Fraud Concerns Trades on a Decentralized Cryptocurrency Network.

As alleged in the Indictment, cryptocurrency is a "digital currency in which transactions are verified, and records are maintained, by a decentralized system using cryptography." Indict. ¶ 4. Cryptocurrency transactions are recorded in units called blocks on a public ledger called a blockchain. *Id.* ¶ 5. The blockchain at issue is called Ethereum, which is a "decentralized blockchain . . . used by millions of people across the world." *Id.* ¶ 7. Ethereum runs on transparent,

[1] Because the Court assumes that allegations in an indictment are true for the purposes of a motion to dismiss, *see United States v. Pierre*, 2023 WL 4493511, at *2 (S.D.N.Y. July 12, 2023), the Peraire-Buenos do the same here, even where they believe the Indictment's allegations misunderstand or misstate the facts, or that the government will not be able to prove its allegations.

open-source computer code that is publicly available for anyone to view and to propose modifications.[2]

"No central actor runs the Ethereum Network." Indict. ¶ 7. Although the Indictment alleges that participants "operate based on a set of rules and protocols," *id.*, and makes allegations about the purported roles and expectations of different players on the Ethereum Network, *see id.* ¶¶ 8-14, the Indictment identifies no governing rules or terms of use that apply to Ethereum users and no source for the alleged roles and expectations.

B. The Alleged Victims' Bots Were Pre-Programmed to Engage in Sandwich Trades.

According to the Indictment, users called validators (1) propose blocks when they are randomly selected, and (2) are "responsible for checking that new blocks are valid before they are added to the Ethereum blockchain." Indict. ¶ 8. To become a validator, a user must "stake," or deposit, 32 ETH (the native cryptocurrency on the Ethereum Network), which can be "slashed" or cut for violations of protocol. *Id.*

The process for adding a block to the Ethereum blockchain sometimes can involve a software program called "MEV-Boost." *Id.* ¶ 11. MEV is short for "maximal extractable value," which is the "maximum value that can be obtained by including, reordering, or excluding transactions when publishing a new block to the blockchain." *Id.* ¶ 10. A validator's use of MEV-Boost to propose blocks and, thus, potentially increase the payout for proposing a block of transactions is optional. *See id.* ¶ 11 (alleging that "90% of Ethereum validators use MEV-Boost"). Like the rest of the software that runs on the Ethereum Network, the MEV-Boost code is "open-

[2] *See What is Ethereum*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-ethereum (last accessed Dec. 5, 2024).

source," *id.*, meaning that anyone can view and propose modifications to it. MEV-Boost was introduced to the Ethereum Network in September 2022, seven months before the alleged fraud.[3]

The Indictment alleges that the process of building and adding a block to the chain pursuant to MEV-Boost occurs through a series of sequential steps. Before the validator proposes a block, users called searchers, builders, and relays have roles to play. *See* Indict. ¶ 11-14. The alleged victims in this case were searchers operating through "automated bots" called "MEV Bots." *Id.* ¶ 13; *see also id.* ¶¶ 17 (defining the "Victim Traders" as "MEV Bots"), 22 (defining the Victim Traders as "searchers who operate MEV Bots"). The searchers "send[] the builder a proposed 'bundle' of transactions" to include in a block. *Id.* ¶ 13. A builder "receives bundles from various searchers and compiles them into a proposed block that maximizes MEV." *Id.* Those potential blocks are subsequently sent to a relay, which submits them to a validator. *Id.*

The alleged victims' MEV Bots had their own profit-seeking instructions. They were programmed to select pending cryptocurrency transactions submitted by other Ethereum users for inclusion in a potential block with an eye towards what the Indictment calls "profitable arbitrage opportunities." *Id.*[4] The MEV Bots allegedly planned to execute this strategy by first identifying another trader's proposed transaction for inclusion in a new block. Indict. ¶ 13.[5] The MEV Bots

---

[3] *See What is MEV-Boost?*, Flashbots, https://docs.flashbots.net/flashbots-mev-boost/introduction (last accessed Dec. 5, 2024) (noting that program was built in connection with the Ethereum Network's transition to "proof of stake"); *The Merge*, Ethereum, https://docs.flashbots.net/flashbots-mev-boost/introduction (last accessed Dec. 5, 2024) (noting that the transition to "proof of stake" system was executed on September 15, 2022). Flashbots is a research and development organization that created the MEV-Boost program.

[4] For reasons elaborated below in support of the Motion to Dismiss the Indictment for Failure to Provide Fair Notice, *see* Section I, *infra*, these actions do not meet any standard definition of arbitrage and in fact are derided in the crypto industry as a form of manipulation. *See also* Motion to Compel Production of *Brady* Material at 6-10 (filed today).

[5] This is possible because "[w]hen a user conducts a transaction on the Ethereum blockchain, such as a buy or sell trade, this transaction is not immediately added to the blockchain" but rather

then would submit a bundle to builders where they sandwich this publicly viewable transaction between newly proposed trades of their own. *Id.* ¶ 13. The first of the MEV Bots' sandwich trades is the searcher's "'frontrun' transaction in which the searcher purchases some amount of cryptocurrency whose value the searcher expects to increase." *Id.* Next comes the pending, authentic transaction requested by the other user. *Id.* The final transaction in the sandwich is the MEV Bots' potential "sell transaction, in which the searcher," through the MEV Bot, "sells the cryptocurrency" that it purchased in the frontrun trade "at a higher price than what the searcher initially paid in order to extract a trading profit." *Id*.

C. The Peraire-Buenos Allegedly Thwart the MEV Bots' Sandwich Trades.

The Indictment alleges that, on April 2, 2023, the Peraire-Buenos obtained $25 million in cryptocurrency by swapping the targeted trades around which the alleged victims' MEV Bots had structured their sandwich trades for different trades before they, as validators, proposed the block. The Indictment calls this the "Exploit," and says it is "believed to be the very first of its kind." *Id.* ¶ 1. Although the Indictment states in conclusory terms that, through the "Exploit," the Peraire-Buenos "stole their victim's cryptocurrency," *id.*, its factual allegations refute this baseless claim. Rather, the allegations demonstrate that the alleged victims' MEV Bots traded their currency away as part of a pre-programmed and ultimately unsuccessful sandwich trade attempt without ever having interacted with the Peraire-Buenos.

1. The alleged victims' MEV Bots propose sandwich trades on the Peraire-Buenos' trades

The Indictment alleges that the Peraire-Buenos began the "Exploit" by proposing eight cryptocurrency transactions. *Id.* ¶ 24. The Indictment calls these the "Lure Transactions" because

"waits alongside other pending transactions in the 'memory pool' or 'mempool,' which is publicly visible." *Id.* ¶ 9.

they were allegedly intended to cause the victims' MEV Bots to target them. *See id.* The Indictment alleges that the MEV Bots attempted to perform sandwich trades involving "particularly illiquid cryptocurrencies" surrounding these eight trades. *See id.*[6] The success of the MEV Bots' strategy of swapping large quantities of cryptocurrencies, only to nearly instantaneously swap the same currencies back again after the user's swap at the center of the sandwich, depended on maintaining the same order of the trades that the MEV Bots sent to the builder. *See* Indict. ¶ 24.

2. The alleged victims' MEV Bots release their proposed sandwich trades

After structuring their proposed transactions as part of their sandwich-trade strategy, the alleged victims' MEV Bots submitted them to a separate user called a builder. *Id.* The builder created a potential block and sent it to another separate user called the relay, which then released the potential block to the validator. *Id.* ¶ 26. There are, thus, at least two users who stand between the searcher and validator. The Indictment does not allege that the validator—either typically or in this case—interacted with the searchers (or the builder) directly or indirectly. The Indictment also does not allege that the MEV Bots had any visibility into, or control over, their proposed sandwich trades once they were released.

3. The Peraire-Buenos' validators allegedly tamper with the potential blocks

The Peraire-Buenos are alleged to have acted as validators with respect to the at-issue transactions. *Id.* ¶¶ 19, 26, 27. When the relay has received potential blocks from builders, the validator typically does not know what transactions are in those potential blocks, but does know

[6] This allegation is false; the transactions at issue involved cryptocurrency tokens that are widely traded on multiple exchanges. *See* Motion to Suppress or, Alternatively, for *Franks* Hearing at 8-9 (filed today).

how much it can expect to be paid for adding a specific block to the blockchain. *See id.* ¶ 13. This information is conveyed by the relay to the validator together with each block's "blockheader." *Id.* After the validator affixes its "digital signature" to a blockheader, "the relay releases the full content of the proposed block." *Id.*

The Indictment alleges that the Peraire-Buenos "exploited a vulnerability in the Relay's computer code by sending the Relay a false signature (the 'False Signature') in lieu of a valid digital signature" which caused the content of a potential block to become visible. *Id.* ¶ 26. The Indictment further alleges that, once the Peraire-Buenos were able to see the full content of the relay's potential block, they "tampered" with the block in the following manner:

First, the Peraire-Buenos allegedly "allowed the Victim Traders to complete their buy transactions (*i.e.*, their frontrun transactions.) In effect, the Victim Traders sold approximately $25 million of [cryptocurrencies] to purchase particularly illiquid cryptocurrencies." *Id.* ¶ 26a. According to the Indictment, through these transactions, the MEV Bots "deposited" the $25 million in cryptocurrencies into "particular liquidity pools" on the Ethereum Network. *Id.* ¶ 26b. In other words, during the first step of the alleged Exploit, the MEV Bots "sold" the allegedly lost currencies to some other user (*i.e.*, not the Peraire-Buenos). The Indictment does not allege that the alleged victims retained any rights to the currencies they traded away in the hope of reaping a profit from their attempted sandwich trades.

Second, the Indictment alleges that the Peraire-Buenos "replaced" the so-called Lure Transactions with new transactions in which the Peraire-Buenos swapped their own holdings of the same cryptocurrencies that the alleged victim searchers' MEV Bots had just bought in their

frontrun trades. *Id.* ¶ 26b.[7] The Indictment calls these the new transactions the "Tampered Transactions," *id.*, but does not explain what "tampered" means in this context.

Third, the Indictment alleges that, "[a]s a result of the[] actions" described above, the MEV Bots' "final sell transactions could not take place" because the MEV Bots' front-running trades had resulted in the purchase of currency that was "effectively worthless." *Id.* ¶ 26c. In other words, the alleged loss occurred through the frontrun trades and could not be recouped by the later sell trades.

ARGUMENT

This case is a far cry from the typical wire fraud prosecution. The Indictment's attempt to shoe-horn its unusual allegations under the rubric of wire fraud fails. The Peraire-Buenos bring three motions to dismiss, each of which, if granted, would dispose of all counts in the Indictment: (1) Motion to Dismiss the Indictment for Failure to Provide Fair Notice; (2) Motion to Dismiss the Indictment for Failure to Allege Essential Elements; and (3) Motion to Dismiss the Indictment as Unconstitutionally Vague. Although these three motions raise independent grounds for dismissal, the failings they identify all stem from the government's misguided attempt to stretch the wire fraud statute to cover allegedly first-of-its-kind conduct.

The first motion presents the threshold constitutional question whether this novel prosecution properly can be brought where there is no prior judicial decision applying the wire

[7] The Indictment elsewhere alleges that the alleged victims' MEV Bots included in their proposed bundles of transactions "coded conditions that the frontrun trades would not be executed unless: (a) the Lure Transactions took place immediately after the frontrun trades; *and* (b) the sell transactions took place immediately after the Lure Transactions." *Id.* ¶ 24. The Indictment does not attempt to square this allegation with its contradictory allegation that the frontrun trades occurred despite the fact that the Lure Transactions did not take place immediately afterwards. Since these are allegedly automated transactions, this should not have been possible. The Indictment does *not* allege that the Peraire-Buenos altered the code that constituted the MEV Bots' proposed sandwich trades.

fraud statute in similar circumstances that would put the Peraire-Buenos on notice that the alleged conduct could be considered criminal. Because the Peraire-Buenos did not have the fair notice the Constitution requires, the wire fraud statute is unconstitutionally vague as applied, and the Indictment must be dismissed. In the alternative, the Indictment must be dismissed for its failure to adequately allege the charged crimes: it omits several essential elements (Motion 2) and otherwise fails to allege facts sufficient to make clear its novel fraud theories (Motion 3). For all these reasons, as elaborated herein, the Court should dismiss the Indictment.

I. MOTION TO DISMISS (1): THE INDICTMENT VIOLATES DUE PROCESS.

A. A Defendant Must Have Fair Notice that His Conduct Is Prohibited.

Under the Due Process Clause of the Fifth Amendment, "[a] statute is unconstitutionally vague if it fails to define the unlawful conduct with sufficient definiteness that ordinary people can understand what conduct is prohibited, or if its vagueness makes the law unacceptably vulnerable to arbitrary enforcement." *United States v. Requena*, 980 F.3d 30, 39 (2d Cir. 2020) (citation omitted). Known as the void-for-vagueness doctrine, this constitutional requirement "addresses concerns about (1) fair notice and (2) arbitrary and discriminatory prosecutions." *United States v. Napout*, 963 F.3d 163, 181 (2d Cir. 2020) (citation omitted).

In evaluating fair notice, "a court must determine whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal." *Id.* (citation omitted). These constitutional protections are paramount in "novel" prosecutions because "due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *United States v. Lanier*, 520 U.S. 259, 266 (1997); *see United States v. Matthews*, 787 F.2d 38, 49 (2d Cir. 1986) (reversing conviction where there was a "lack of any precedent for the Government's theory of liability"); *United States v. Saathoff*, 708 F. Supp. 2d

1020, 1036-37 (S.D. Cal. 2010) (dismissing fraud charges because of "the novelty" of the government's theory and the "vagueness of the text of the statute").

The wire fraud statute, which criminalizes "scheme[s] or artifice[s] to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises," 18 U.S.C. § 1343, is particularly susceptible to prosecutorial overreach. *See United States v. Czubinski*, 106 F.3d 1069, 1079 (1st Cir. 1997). While the wire fraud statute "can address new forms of serious crime that fail to fall within more specific legislation," its "broad language" can also "be used to prosecute kinds of behavior that, albeit offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected by the instigators to form the basis of a federal felony." *Id.* For that reason, in other contexts, the Supreme Court has repeatedly rejected aggressive applications of the federal fraud statutes based on vagueness and related federalism concerns. *See Ciminelli v. United States*, 598 U.S. 306, 315 (2023) (reversing wire fraud conviction where the government's theory would "make[] a federal crime of an almost limitless variety of deceptive actions traditionally left to state contract and tort law"); *Skilling v. United States*, 561 U.S. 358, 408-09 (2010) (limiting the scope of 18 U.S.C. § 1346, which criminalizes honest-services fraud, in order to avoid "due process concerns underlying the vagueness doctrine"); *McNally v. United States*, 483 U.S. 350, 360 (1987) (limiting the scope of mail fraud statute to tangible property to avoid "constru[ing] the statute in a manner that leaves its outer boundaries ambiguous").

B. The Indictment's Novel Theories Are Unconstitutional.

Nothing in the text of the wire fraud statute nor the cases that have construed it provided the Peraire-Buenos with fair notice that the alleged conduct could constitute wire fraud. The Indictment itself acknowledges that the circumstances of this case are novel, involving conduct

that is "believed to be the very first of its kind." Indict. ¶ 1. This concession all but dooms the Indictment. Where the "core factual scenario as alleged in th[e] indictment concerns conduct that is not even close to the facts of any other reported judicial decision," the Peraire-Buenos "would be denied their Fifth . . . Amendment rights to fair notice should a trial be permitted." *Saathoff*, 708 F. Supp. 2d at 1034. But even the concession that the alleged conduct is "the very first of its kind" seriously understates the novelty of this prosecution. Several features of this case underscore the degree to which the government is inappropriately attempting to push the wire fraud statute into uncharted territories.

First, this Indictment is an unusual government intervention into the Ethereum Network, which is decentralized and "trustless" by design. In particular, this case concerns the in-the-weeds expectations of various users of a particular open-source computer software (MEV-Boost). The prosecution's novel theory poses complicated questions: what are Ethereum "validators" who elect to use MEV-Boost permitted to do; do "validators" owe duties to "searchers," even though those parties play distinct roles, do not contract, and never communicate; and if validators breach those newly-identified duties, does that equate to a scheme to defraud within the meaning of the federal fraud statutes? No government regulation has sought to answer these novel and controversial questions. It is fundamentally unfair for the United States government to regulate for the first time ***through criminal prosecution*** the rights and duties of searchers and validators on the Ethereum Network. *Cf. United States v. Giffen*, 326 F. Supp. 2d 497, 506 (S.D.N.Y. 2004) (holding honest services wire fraud statute vague as applied where "there are no published decisions addressing the honest services theory the Government espouses in this case").

Indeed, the very structure of the Ethereum Network—which is decentralized, trustless, and utilizes economic incentives to encourage behavior among profit-seeking users—is in tension with

the criminal prosecution of users operating pursuant to transparent protocols that the Ethereum community has stablished. The Indictment recognizes that the MEV-Boost program's software was "open-source," Indict. ¶ 11, meaning its code was publicly visible. The Indictment further notes that the "rules and protocols" at play on the Ethereum Network "are typically executed through 'smart contracts.'" *Id.* ¶ 7. The Indictment acknowledges that "smart contracts" are "self-executing computer protocols with if/then conditions—which enable transactions to take place on the Ethereum blockchain without the need for a trusted intermediary," *id.*, but it ignores that they are also publicly visible and "guaranteed to execute according to the rules defined by [their] code, which cannot be changed once created." *Introduction to smart contracts*, Ethereum (Mar. 7, 2024), https://ethereum.org/en/smart-contracts/. A benefit "of a smart contract is that it deterministically executes unambiguous code when certain conditions are met." *Id.* Whereas "traditional contracts are ambiguous because they rely on humans to interpret and implement them[,] . . . smart contracts execute precisely based on the conditions written within the contract's code." *Id.* In this way, Ethereum users have purposefully structured a system where adversarial trading can occur without the need to place trust in a counterparty, interpret the counterparty's actions, or guess at its intentions. Instead, completely transparent contracts, and the software and protocols that facilitate them, determine what happens and when. To the extent issues arise, the Ethereum Network provides for economic incentives to encourage or discourage behavior. *See*, *e.g.*, Indict. ¶ 8 (noting that certain conduct by validators is discouraged by providing that "the staked ETH" will be "'slashed' or cut").

In this context, a criminal prosecution for actions allowed by the very code that set the parameters of what users in a decentralized and trustless market can do is wholly unexpected. That the government would charge such a case as wire fraud is equally surprising where the underlying

code that permitted the alleged "Exploit" was as visible to the alleged victims' MEV-Bots as to the Peraire-Buenos and where the Peraire-Buenos are not alleged to have made any representations (let alone misrepresentations) to the alleged victims either directly or indirectly. Under this factual scenario, if fraud is to occur it must be due to the violation of some other obligation imposed on Ethereum validators—but the Indictment does not allege any such obligation. At a minimum, where everyone on the exchange has access to the same information on which to base their adversarial trading strategies, it cannot be said that it was "reasonably clear at the relevant time that the [alleged] conduct" permitted by the relevant code could be considered fraudulent. *Napout*, 963 F.3d at 181 (citation omitted).[8]

This is not to say that crimes occurring in or related to cryptocurrency markets are not (or should not be) prosecuted. The headlines are replete with stories on criminal cases relating in some way to cryptocurrency markets. But these prosecutions have tended to be based on theories of illegality that are akin to well-established financial crimes committed in traditional financial markets. For example, the crimes charged in the aftermath of the collapse of FTX alleged straightforward fraud and misuse of customer funds in a circumstance where the companies and their officers owed disclosure duties and made false statements to the alleged victims. *See* Superseding Indict., *United States v. Bankman-Fried*, S5 22-cr-673-LAK (S.D.N.Y. Mar. 28, 2023), ECF 115 (alleging a scheme to "access and steal FTX customer deposits without detection" and making "false representations to potential investors about the source of the multi-billion dollar hole in FTX's balance sheet"). Kristijan Krstic and others were charged with conspiring to create

[8] To be clear, this Motion does not rely upon what has been characterized as a "code is law" argument, the most expansive versions of which contend that something cannot be illegal if it is permitted by the relevant computer code. Actions permitted by the code of a cryptocurrency exchange potentially could be illegal in various ways. For example, the conduct could contravene some other government regulation. The Indictment cannot and does not allege this situation.

fake crypto trading platforms where investors "were shown a positive return on their investments" where "no real trading was actually occurring, and their investment funds were being spent on personal expenses and to pay commissions." Superseding Indict., *United States v. Krstic et al.*, No. 3:20-cr-120-B (N.D. Tex. Feb. 5, 2021), ECF 37. Avi Eisenberg was charged with fraud because he allegedly manipulated a cryptocurrency market with a pump-and-dump-type scheme in which he artificially inflated token prices and then borrowed based on false pretenses. *See* U.S. Br. in Opp'n to Mot. to Dismiss, *United States v. Eisenberg*, No. 23-cr-10-AS (S.D.N.Y. Aug. 25, 2023), ECF 36 (describing the alleged fraud as centering on "massive purchases to artificially inflate the price" of a cryptocurrency). This case, by contrast, has no obvious analogue to fraud or market manipulation cases in traditional or even digital markets.

Second, at the time of the purported "Exploit," the vaguely described protocols or norms that the Peraire-Buenos allegedly violated were in flux in critical ways that the Indictment elides. In September 2022, just six months prior to the supposedly fraudulent transactions, Ethereum had affected a major change when it switched its consensus protocol from a "proof of work" to a "proof of stake" system, a change which effectively created the role of the validator. *See* Shalini Nagarajan and Sebastian Sinclair, *Ethereum Switches to Proof-of-stake After 7 Years of Work*, Blockworks (Sept. 15, 2022), https://blockworks.co/news/ethereum-switches-to-proof-of-stake-after-7-years-of-work. MEV-Boost was launched at the same time. *See* p. 5, *supra*. As noted above, and as alleged in the Indictment, MEV-Boost is an optional tool that validators can use to maximize their own profits. *See* p. 4, *supra*; Indict. ¶ 11. Since launching in September 2022, the MEV-Boost program has undergone at least 13 releases.[9] Flashbots, the developers of the first relay, have also repeatedly revised the roles of relay and builder, updating the software with new

[9] *See* https://github.com/flashbots/mev-boost/releases?page=1. (last accessed Dec. 3, 2024).

features such as the introduction of a fast-track queue for high-priority builders.[10] Other users have proposed their own open-source versions of the relay that differ in a variety of respects from the initial Flashbots version.[11] Just recently, a comprehensive overhaul of the Ethereum Network was proposed.[12] The Indictment ignores the experimental nature of Ethereum's protocols, which undermines the very existence of any clear, stable, and well-known "rules" that the Peraire-Buenos supposedly violated.

Third, even if fraud could occur as alleged in the Indictment, this case is a strange and unexpected foray for the government into policing transactions among sophisticated parties on decentralized cryptocurrency markets because the alleged victims were engaged in market-manipulating sandwich attacks. Although the Indictment characterizes the alleged victims' MEV-Bots as pursuing "arbitrage opportunities," that does not accurately describe their strategy which created the very price discrepancies they aimed to profit from. In the crypto industry, these actions are understood as a form of market manipulation called "sandwich attacks."[13] *See* Motion to Compel Production of *Brady* Material at 6-10 (filed today). According to the Indictment, the Peraire-Buenos were the MEV Bots' intended targets. The alleged victims hoped to front-run the Peraire-Buenos' trades, manipulate the price of the cryptocurrencies the Peraire-Buenos were

---

[10] *See* https://github.com/flashbots/mev-boost-relay/releases?page=1. (last accessed Dec. 3, 2024).

[11] *See, e.g.*, https://github.com/michaelneuder/optimistic-relay-documentation/tree/main (last accessed Dec. 3, 2024).

[12] *See* James Hunt and Danny Park, *Justin Drake proposes 'Beam Chain,' an Ethereum consensus layer redesign*, The Block (Nov. 12, 2024), https://www.theblock.co/post/325715/justin-drake-ethereum-beam-chain.

[13] *See What are sandwich attacks in crypto?*, Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-are-sandwich-attacks-in-crypto#:~:text=A%20sandwich%20attack%20is%20a,%22sandwiching%22%20the%20user's%20transaction (last accessed Dec. 3, 2024).

going to buy, and then backrun those trades to capture the resulting profits (*i.e.*, selling back the same cryptocurrencies that they purchased just two transactions earlier at a lower price).

The government has long viewed such activity as manipulative and, in certain circumstances, even criminal. *See United States v. Mahaffy*, 693 F.3d 113, 138 (2d Cir. 2012) (noting that "illegality occurred when the defendants bought and sold securities as part of a scheme involving illegal bribery and frontrunning"); *United States v. Frayler*, 2000 WL 174958, at *2 (S.D.N.Y. Feb. 15, 2000) (noting that defendant pleaded guilty to "the familiar securities fraud of 'front running'"); Superseding Indict., *United States v. Taub*, No. 2:18-cr-79-JMV (D.N.J. Oct. 23, 2019), ECF 86 (alleging securities fraud where defendant "engaged repeatedly in a series of contemporaneous transactions designed to artificially influence the market price of securities" and to convey "false impression that there was real market interest in the securities" when there was not); *cf.* Indict., *United States v. Eisenberg*, No. 23-cr-10-AS (S.D.N.Y. Jan. 9, 2023), ECF 4 (charging a market manipulation scheme occurring in a crypto market).

But the government has yet to prosecute entities, like the alleged victims here, that perpetrate "sandwich attacks" on the Ethereum Network or other cryptocurrency networks. Many commentators in the cryptocurrency community consider "sandwich attacks" to be manipulative, unlawful, and even criminal.[14] Thus, until this case broke new ground, a reasonable inference from the government's conspicuous inaction regarding sandwich attackers was that the

[14] *See also* Damilola Atobatele, *Understanding Sandwich Attacks in DeFi: How to Protect Your Investments*, DeFi Planet (July 19, 2023), https://defi-planet.com/2023/07/understanding-sandwich-attacks-in-defi-how-to-protect-your-investments/ (noting that sandwich attacks "are generally illegal within traditional systems and may also be prohibited in the DeFi space once regulatory measures are implemented"); Darren Kleine, *Sandwich Attacks: Stealing or Just Playing the DeFi Game?*, Blockworks (May 19, 2023), https://blockworks.co/news/sandwich-attack-mev-ethereum (noting that "[i]n the traditional finance world," sandwich attacks "would likely be a clear-cut case of illegal behavior").

government did *not* view intervention in adversarial trading on decentralized cryptocurrency exchanges like Ethereum as appropriate, even where there were well-recognized analogues to illegal behavior in traditional markets. It is especially unusual that the government's first prosecution of this type would be on the behalf of the very predatory entities it typically prosecutes in other contexts.

Fourth, the government also has not prosecuted other attempts to *counter* sandwich trades. In the crypto community, these strategies are no secret but rather are openly commented upon and even lauded as an example of how economic consequences and not government regulation can incentivize behavior on decentralized exchanges. In one well-known example, a trader on the Ethereum blockchain, who wished to "illustrate to novice traders the risks of playing in the mempool," employed a new strategy to "turn[] the tables on" sandwich traders. *See Wrecking sandwich traders for fun and profit*, https://github.com/Defi-Cartel/salmonella (last accessed Dec. 3, 2024).[15] The trader created a new cryptocurrency token named Salmonella. *Id.* While this new token "behave[d] exactly like" other tokens on the Ethereum Network in most regards, the trader added code "to detect when anyone other than the specified owner is transacting it and in these situations . . . only return[] 10%" of the expected payout despite sending misleading signals suggesting a full return. *Id.* The trader opened a "trap" liquidity pool containing his Salmonella token and created "a series of bait transactions" with the Salmonella token that "would look like juicy opportunities" to entice sandwich traders. *Id.* When traders attempted to sandwich those bait transactions,

> '[i]nstead of giving them a juicy payout, the token itself in the trade exploits the sandwich trader by giving them only a fraction of the tokens they thought the swap would yield,' [the trader] explained. 'After this happens, the 'sell' order of the

[15] This trader was so confident that his behavior was not criminal that he drafted an explanation of his anti-sandwiching strategy and posted it online for public consumption.

> sandwich trader now fails and they are left holding the Salmonella token. Instead of making a bunch of ETH in profit from my bait, they are instead left with a stomach full of Salmonella.'

William Foxley, *Bad Sandwich: DeFi Trader 'Poisons' Front-Running Miners for $250K Profit*, CoinDesk (Sept. 14, 2021), https://www.coindesk.com/tech/2021/03/22/bad-sandwich-defi-trader-poisons-front-running-miners-for-250k-profit/. Speaking to the press, the trader expressed no regrets and said that trading on the Ethereum blockchain "is a game of high-stakes poker and [the sandwich traders] sat down at the table intending to take all of my chips. Maybe next time they will be the ones walking home with all my chips. That's the game[.]" *Id.*[16] This trading strategy does not appear to have resulted in a prosecution, nor did the actions of others who replicated the strategy. In this context, it was reasonable for the Peraire-Buenos to understand that the wire fraud statute did not apply to alleged attempts by a potential victim to thwart a manipulative sandwich attack.

In charging this case as a fraud case and trumpeting its novelty in the Indictment's prefatory paragraphs, the government is taking a bold step. For the reasons set forth above, that step is seriously misguided. At a minimum, its novelty defies the Due Process Clause and requires dismissal of this first-of-its-kind case.

---

[16] Something akin to this scenario occurred when a Salmonella victim (itself a sandwich attacker) devised a similar strategy that "ended up successfully baiting many more sandwichers." https://x.com/bertcmiller/status/1381296111181299713 (last accessed Dec. 5, 2024). Bert Miller of Flashbots (the entity that created MEV-Boost) commented that the episode demonstrated that "[i]n a short period of time the victim turned into an apex predator," *id.*, and that "even those who think they are predators might turn out to be prey," https://x.com/bertcmiller/status/1381296117925740547 (last accessed Dec. 5, 2024).

II. MOTION TO DISMISS (2): THE INDICTMENT FAILS TO STATE THE ESSENTIAL ELEMENTS OF THE WIRE FRAUD CHARGES.

Even if wire fraud could be charged in this context consistent with the Fifth Amendment, the Indictment here does not adequately do so because it omits several essential elements of the offense. The Indictment Clause of the Fifth Amendment and the Notice Clause of the Sixth Amendment require that an indictment allege every element of the offense charged. *United States v. Pirro*, 212 F.3d 86, 91-92 (2d Cir. 2000). While an indictment reciting an offense's statutory language often will capture its core elements, that is not true for offenses with "implicit" elements. *Id.* at 93. For such offenses, an indictment that "tracks the language of the statute and fails to allege the implicit element explicitly . . . fails to allege an offense." *Id.* at 93 (quoting *United States v. Foley*, 73 F.3d 484, 488 (2d Cir. 1996), *abrogated on other grounds by United States v. Santopietro*, 166 F.3d 88, 92-93 (2d Cir. 1999)) (internal quotation marks omitted).

Dismissal is appropriate where the allegations in an indictment would not support a conviction if proven beyond a reasonable doubt because they fail to allege an essential element, implicit or otherwise. *See, e.g.*, *Pirro*, 212 F.3d at 95 (affirming partial dismissal of indictment for failure to allege the source of the duty to disclose that had allegedly been violated); *United States v. Berlin*, 472 F.2d 1002, 1008 (2d Cir. 1973) (dismissing counts in indictment for failure to allege defendant's knowledge of supposedly false statements); *see also* Fed. R. Crim. P. 12(b)(3)(B)(v) (court may dismiss an indictment pretrial for "failure to state an offense").

The elements of wire fraud under 18 U.S.C. § 1343 are "(1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the mails or wires to further the scheme." *United States v. Weaver*, 860 F.3d 90, 94 (2d Cir. 2017) (per curiam) (citation omitted). A scheme to defraud requires a "misrepresentation or concealment of a material fact." *Neder v. United States*, 527 U.S. 1, 22 (1999) (emphasis omitted); *see also id.* at 20 (concluding that the federal "fraud

statutes . . . require that a 'scheme to defraud' employ material falsehoods" (emphasis omitted)). The victim also must possess an enforceable property right. *See United States v. Pierce*, 224 F.3d 158, 165-66 (2d Cir. 2000). Finally, the defendant must act with an intent to defraud, not merely an intent to deceive. *See United States v. Starr*, 816 F.2d 94, 98 (2d Cir. 1987).[17]

The Indictment in this case fails to allege several of these essential elements. First, the Indictment fails to allege any material misrepresentation or omission by the Peraire-Buenos. Second, the Indictment does not allege the deprivation of any traditional property right of the alleged victims. Finally, the Indictment alleges no intent to defraud because the supposed deceit did not go to the nature of the bargain as it did not prevent the alleged victims from having the transactions they proposed executed as programmed. Absent allegations on these key elements of the charged offenses, the Indictment fails to charge wire fraud or conspiracy to commit wire fraud.

A. The Indictment Fails to Allege a Material Misrepresentation or Omission.

The Indictment does not allege any (1) materially false or misleading statement or (2) material omission with a duty to disclose. The first element of wire fraud, a "scheme to

[17] The same requirements pertain to a conspiracy to commit wire fraud under 18 U.S.C. § 1349. A conspiracy conviction requires an agreement to engage in conduct that "includes all the elements of the substantive crime[s]." *United States v. Pinckney*, 85 F.3d 4, 8 (2d Cir. 1996) (citation omitted). A failure of proof on an essential element of the underlying offense dooms a conspiracy conviction. *See id.* (failure to prove interstate commerce element of underlying offense required acquittal on conspiracy count). And while an indictment need not allege the object of a conspiracy with the same "technical precision" as when it charges the substantive offense, *United States v. Bout*, 731 F.3d 233, 240 (2d Cir. 2013), failure to allege an essential element of the substantive offense will mandate dismissal of a related conspiracy charge, *see, e.g.*, *United States v. Case*, 2007 WL 1746399, at *6 (S.D. Miss. June 15, 2007) (dismissing wire fraud conspiracy charge to the extent it relied on vague fraud allegations that failed to allege a material misrepresentation); *United States v. Higgins*, 511 F. Supp. 453, 456 (W.D. Ky. 1981) (dismissing substantive fraud charges for failure to state an offense and concluding conspiracy charge "must also fall, because it charges a conspiracy which has no illegal object as an underlying offense" (citing *United States v. Aloi*, 511 F.2d 585, 592 (2d Cir. 1975)). The arguments against the wire fraud charge in Count Two apply with equal force to the conspiracy charge in Count One.

defraud," requires "fraudulent or deceptive means, such as material misrepresentation or concealment." *Ctr. Cadillac, Inc. v. Bank Leumi Trust Co.*, 808 F. Supp. 213, 227 (S.D.N.Y. 1992) (citation omitted), *aff'd* 99 F.3d 401 (2d Cir. 1995). The government must prove that the defendant engaged in a deceptive course of conduct through a "misrepresentation or concealment of material fact." *Neder*, 527 U.S. at 22 (emphasis omitted); *see United States v. Autuori*, 212 F.3d 105, 115, 118 (2d Cir. 2000) (wire fraud statute criminalizes "affirmative misrepresentations," "omissions of material information that the defendant has a duty to disclose," and/or misleading "half-truths" that omit facts necessary to make the statements "not misleading" (citation omitted)); *see also United States v. Radley*, 632 F.3d 177, 185 (5th Cir. 2011) ("Although the language of § 1343 does not require a material misrepresentation [or omission], the Supreme Court has interpreted the statute to call for one." (citing *Neder*, 527 U.S. at 20-25)).

1. No Valid Omission Theory

The Indictment does not allege a valid omission theory. An omission can be equivalent to a misrepresentation when there is a duty to disclose. *United States v. Szur*, 289 F.3d 200, 211 (2d Cir. 2022). Such a duty "arises [only] when one party has information that the other [party] is entitled to know because of a fiduciary or other similar relation of trust and confidence between them." *Id.* (quoting *Chiarella v. United States*, 445 U.S. 222, 228 (1980)) (internal quotation marks omitted) (alterations in original). The Indictment alleges no such duty or special relationship between the Peraire-Buenos, as "validators" or "traders," and the alleged victims, as "searchers." This makes sense: as described in the Indictment, validators, traders, and searchers in the MEV-Boost process do not interact, and the Ethereum Network, a trustless, decentralized blockchain, incentivizes the behavior of all participants through economic consequences, not formal disclosure duties. *See also* Section I, *supra*. The Indictment's failure to allege any duty to

disclose in the Indictment precludes the prosecution's reliance on an omission theory. *See, e.g.*, *Pirro*, 212 F.3d at 93, 95 (affirming partial dismissal of indictment premised on an omission theory when it alleged an omission but not "the crucial background fact that gives rise to the duty to disclose the fact that was omitted").

2. No Valid Misrepresentation Theory

The Indictment also does not sufficiently allege any material misrepresentation. The Indictment identifies at most two alleged "material misrepresentations"—the so-called "Lure Transactions" and the "False Signature." Indict. ¶¶ 35, 37. However, as alleged, neither constitutes a material misrepresentation under the wire fraud statute. *See also* Section III, *infra* (noting Indictment is unconstitutionally vague). "The absence of any allegations of misrepresentation is fatal to the government's wire fraud counts, and they must be dismissed." *United States v. Radley*, 659 F. Supp. 2d 803, 820 (S.D. Tex. 2009), *aff'd*, 632 F.3d 177 (5th Cir. 2011).

The "Lure Transactions." Beginning with the so-called "Lure Transactions," the Indictment alleges only that the Peraire-Buenos submitted "at least eight specific transactions" that "cause[d] the [alleged victims'] MEV Bots to propose approximately eight bundles that included the Lure Transactions." Indict. ¶ 24. The Indictment does not say anything about the content of the Lure Transactions (other than saying they were cryptocurrency transactions), nor does it describe what information they may have conveyed to the MEV Bots or what was supposedly false or misleading about that information. There is no allegation that Lure Transactions were not *bona*

fide proposed cryptocurrency trades the Peraire-Buenos honestly offered and ultimately executed.[18]

The "False Signature." The alleged "False Signature" similarly fails to constitute a material misrepresentation. Although the Indictment labels as "false" the digital signature[19] that the Peraire-Buenos allegedly sent to the relay, it does not explain how a validator's signature could be false or what information a digital signature conveys. Rather, the Indictment alleges only that (a) the Peraire-Buenos "knew that the information contained in the False Signature could not be verified for ultimate publication to the blockchain" and that (b) the False Signature "trick[ed] the Relay to prematurely release the full content of the proposed block." Indict. ¶ 26. But these sparse allegations say nothing about how the signature at issue in this case was false or misleading. And if the signature was allegedly misleading because it omitted certain information supposedly necessary to make it not misleading, the Indictment does not say what information was omitted. The Indictment conspicuously fails to allege that a validator is under any duty to ensure its signature could, in fact, be "verified for ultimate publication to the blockchain."

Nor does the Indictment allege how the signature "tricked" the relay, which the Indictment admits is merely a program operating pursuant to "open source code" publicly available for anyone to view. *See id.* (alleging only that the Peraire-Buenos "exploited a vulnerability in the Relay's computer code"). If, as these allegations appear to concede, the relay's publicly viewable code

---

[18] All of the alleged Lure Transactions were subsequently added to blocks on the Ethereum blockchain. *See* Motion to Suppress or, Alternatively, for *Franks* Hearing at 5-8 (filed today).

[19] A digital signature within the MEV-Boost system, as relevant here, is distinct from a traditional signature of one's name on a document—even a traditional digital signature—in various ways, including with respect to what information it potentially could contain. Because the Indictment fails to allege the function and structure of digital signatures generally, or the content of the alleged False Signature, the distinction between digital and analogue signatures is immaterial to this Motion.

permitted it to release the information to the validator in the manner alleged, then such a disclosure cannot be a "trick" or the consequence of fraud.

Finally, the "False Signature" cannot have been a material misrepresentation within the meaning of the wire fraud statue for the additional reason that it could have had no role in causing the alleged victims to part with their money. The wire fraud statute "requires that the defendant's fraud be 'the mechanism naturally inducing [the victim or the victim's custodian] to part with money.'" *United States v. Berroa*, 856 F.3d 141, 149 (1st Cir. 2017) (quoting *Loughrin v. United States*, 573 U.S. 351, 365 (2014)). This causation requirement is an additional, implicit element of the offense that derives from the text of the wire fraud statute, which requires that money or property be obtained "by means of" a fraudulent statement. *Id.*; *see Loughrin*, 573 U.S. at 362-66; 18 U.S.C. § 1343.[20] Here, the allegedly False Signature could not have "induced" the alleged victims' MEV-Bots to part with their cryptocurrencies because, according to the Indictment, they already traded those currencies away through their pre-programmed frontrun trades when the False Signature was allegedly conveyed. *See* Indict. ¶ 26; *see* pp. 8-9, *supra*. Nor is there any allegation that the relay, which the Indictment recognizes is a computer program, *see* Indict. ¶ 26, held the cryptocurrencies as the alleged victims' custodian. According to the Indictment, the alleged victims' MEV Bots sold the currencies at issue in the frontrun trades directly into liquidity pools on the Ethereum Network. *See id.* ¶ 26b; *see also* pp. 8-9, *supra*. The relay is not alleged to have had any contact with the allegedly lost currencies. Accordingly, because the alleged False Signature could not and did not induce the alleged victims or anyone else to part with the at-issue

[20] While *Loughrin* concerned the bank fraud statute, the mail and wire fraud statutes contain the same "by means of language" and thus the same causation requirement. *See Berroa*, 856 F.3d at 150-54 (vacating mail fraud convictions for failure of proof on *Loughrin* causation element).

cryptocurrencies, it cannot be a material misrepresentation within the meaning of the wire fraud statute.

B. The Indictment Fails to Allege the Deprivation of a Traditionally Recognized, Enforceable Property Right.

The Indictment must be dismissed for the independent reason that it fails to allege the deprivation of a "traditionally recognized, enforceable property right." *United States v. Henry*, 29 F.3d 112, 115 (3d Cir. 1994). "A scheme to deceive, however dishonest the methods employed, is not a scheme to defraud in the absence of a property right for the scheme to interfere with." *Pierce*, 224 F.3d at 165. The wire fraud statute covers only schemes to deprive another of rights that have "long been recognized as property when the wire fraud statute was enacted." *Ciminelli*, 598 U.S. at 314 (citation omitted).

Courts have held that a wide array of valuable interests fall outside the scope of the traditional property rights that the federal fraud statutes protect where the victim lacks an enforceable claim to the property. *See, e.g.*, *United States v. Adler*, 186 F.3d 574, 578, 580 (4th Cir. 1999) (unsecured creditor's interest in debtor's property); *United States v. $52,037.96 seized*, 2015 WL 5601848, at *7-8 (D. Conn. Sept. 23, 2015) (future market share); *Pharmacare v. Caremark*, 965 F. Supp. 1411, 1417-19 (D. Haw. 1996) (same); *Roitman v. New York City Transit Auth.*, 704 F. Supp. 346, 348-49 (E.D.N.Y. 1989) (potential employment as a teacher). In these cases, the fact that the victims did not have "a contractual right to the [property] in question," *Adler*, 186 F.3d at 580, or held "no more than expectation of" the property, *Roitman*, 704 F. Supp. at 349, meant that the alleged interference with that interest (however deceptive) fell outside the reach of the wire fraud statute.

Henry is instructive. The fraud charges there concerned the "alleged corruption of the process by which banks were chosen to be the depositories" for a public agency's revenues. 29

F.3d at 113. The government claimed the banks who were not selected as depositories were victims. *See id.* In affirming dismissal of the indictment, the Third Circuit first concluded that the banks bidding on deposits in a rigged auction did not have an enforceable right to the deposits because "[e]ven in a fair process, [the prevailing bank] might still have won the deposits." *Id.* at 115. The court framed the relevant "issue" as "whether the competing banks' interest in having a fair opportunity to bid for something that would become their property if and when it were received" was a property right "for purposes of the fraud statutes." *Id.* The court concluded it was not. *Id.* The court noted that the banks' interest in a fair process was "valuable," but not "a traditionally recognized, enforceable property right." *Id.* Importantly, the court reasoned that, even if the fair bidding process was viewed as "a promise to the bidding banks from those in charge of the process that they would not interfere with it," that promise still was not "traditional property." *Id.*

Here, the Indictment fails to allege a "traditionally recognized, enforceable property right." *Id.* True, the Indictment alleges that the victims lost money (in the form of cryptocurrencies). *E.g.*, Indict. ¶ 1. But focusing on the underlying transactions, the Indictment alleges that the alleged victims' automated MEV Bots traded *away* the cryptocurrencies they owned through risky frontrun trades in an effort to manipulate the relative values of those cryptocurrencies. *See* pp. 8-9, *supra*. These trades were pre-programmed before any alleged "tampering" with the order of the transactions on the potential block by the Peraire-Buenos. Indict. ¶ 26b (alleging "the Victim Traders had *recently purchased*" cryptocurrencies through the frontrun transaction before the "Tampered Transactions" took place). The Indictment further alleges that the frontrun transactions were executed as the alleged victims' MEV Bots had proposed. *Id.* ¶ 26a. By trading away their cryptocurrencies with no guarantee that their manipulative strategy would yield profits, the alleged

victims forfeited their existing property rights in their existing cryptocurrencies for an *expectation* of future financial gain dependent on events outside of their control. This contingent property "interest" (if it even is one) is not cognizable under the wire fraud statute.

C. The Indictment Does Not Allege an Intent to Defraud.

Finally, the Indictment does not allege that the Peraire-Buenos acted with intent to defraud the alleged victims because the alleged victims received what they bargained for and because the Peraire-Buenos are not alleged to have made any misrepresentations with respect to that bargain. "Essential to a scheme to defraud is fraudulent intent." *United States v. D'Amato*, 39 F.3d 1249, 1257 (2d Cir. 1994). The law distinguishes between intent to deceive and intent to defraud, and the Second Circuit has vacated fraud convictions where the victims were deceived into a course of action but ultimately not defrauded because they received the product or service they bargained for. *See, e.g.*, *Starr*, 816 F.2d at 98-99, 101; *see also United States v. Shellef*, 507 F.3d 82, 108 (2d Cir. 2007) (distinguishing "schemes that do no more than cause their victims to enter into transactions they would otherwise avoid," which are not wire fraud, from "schemes that depend for their completion on a misrepresentation of an essential element of the bargain," which may be).

Here, the alleged victims' MEV Bots got precisely what they bargained for in their trades on the Ethereum blockchain. The Indictment alleges that through the frontrun trades, the "Victim Traders sold approximately $25 million of various stablecoins or other more liquid cryptocurrencies to purchase particularly illiquid cryptocurrencies." Indict. ¶ 26a. It further alleges that the later sell trades would have then been canceled as a result of the MEV Bots' own code, which were programmed to abort the transaction if certain conditions were not met, *see id.*

¶ 24,[21] akin to a fill-or-kill order on a traditional exchange. The MEV Bots allegedly expected that as a result of their two transactions, and contingent on those transactions' relative position to the "Lure Transactions," they would profit through split-second changes in the relative values of the swapped currencies. *See* pp. 5-7, *supra*. Although that profit opportunity was not realized, the alleged victims' MEV Bots' two transactions in search of that opportunity were executed (or not) as they were programmed. *See* Indict. ¶ 24. And, for the reasons already explained, *see* Section II.A, *supra*, the Peraire-Buenos are not alleged to have made a misrepresentation relating to the MEV Bots' sandwich strategy. In light of these allegations, the Indictment does not allege the requisite intent to defraud to support the wire fraud charges.

III. MOTION TO DISMISS (3): THE INDICTMENT IS UNCONSTITUTIONALLY VAGUE.

In the alternative to Motion to Dismiss (2), the Court should dismiss the Indictment because its failure to allege facts bearing on the essential "scheme to defraud" element violates the Fifth and Sixth Amendments to the Constitution. In addition to alleging the essential elements, an indictment also must contain "*the essential facts* constituting the offense charged." *United States v. Seeger*, 303 F.2d 478, 483 (2d Cir. 1962) (quoting Fed. R. Crim. P. 7(c)) (internal quotation marks omitted)). This requirement serves "three constitutionally required functions": (1) it "fulfills the Sixth Amendment right to be informed of the nature and cause of the accusation"; (2) "it prevents a person from being subject to double jeopardy as required by the Fifth

[21] The Indictment is unclear regarding the conditions necessary for the sell trades to occur as programmed and the reason they were not completed. Paragraph 26(c) of the Indictment alleges that the MEV Bots' sell trades did not occur because the liquidity pools had been "drained." But, according to other allegations in the Indictment, the MEV Bots' code would not have permitted those sell trades to occur if a transaction *other* than the target of the MEV Bots' sandwich—the Lure—followed the frontrun. *Id.* ¶ 24; *see also* n.7, *supra*. For purposes of this Motion, this ambiguity is immaterial because in either scenario the sell trades' pre-programmed logic cancelled the trade.

Amendment"; and (3) "it serves the Fifth Amendment protection against prosecution for crimes based on evidence not presented to the grand jury." *United States v. Walsh*, 194 F.3d 37, 44 (2d Cir. 1999) (internal quotation marks omitted).

An indictment that fails to allege facts sufficient to "apprise the defendant 'with reasonable certainty[] of the nature of the accusation against him is defective'" and must be dismissed. *Russell v. United States*, 369 U.S. 749, 765 (1962) (quoting *United States v. Simmons*, 96 U.S. 360, 362 (1877)) (alterations omitted); *see, e.g.*, *United States v. Mariani*, 90 F. Supp. 2d 574, 586-88 (M.D. Pa. 2000) (precluding government from pursuing theories of property deprivation "not specified in the indictment"); *United States v. Telink, Inc.*, 702 F. Supp. 805, 809 (S.D. Cal. 1988) ("Money or property loss is an essential element of [wire fraud], and this element is not described sufficiently to put the defendants on notice and to allow preparation of a defense.").

Notwithstanding its lengthy background allegations, the Indictment entirely disregards the subject that is "central to every prosecution" under the wire fraud statute, *Russell*, 369 U.S. at 764—the alleged false or misleading statements. As discussed above, *see* pp. 21-23, *supra*, a material misrepresentation or omission is a key element of a wire fraud offense. For the reasons set forth above in connection with the Motion to Dismiss the Indictment for Failure to Allege Essential Elements, the Indictment's conclusory allegations regarding the so-called "Lure Transactions" and "False Signature" are insufficient to charge a material misrepresentation or omission that would qualify under the wire fraud statute. But even if the Indictment adequately stated the material misrepresentation or omission element in superficial terms simply by using the words "lure" or "false," the lack of factual elaboration renders the charges unconstitutionally vague.

Start with the so-called "Lure Transactions." The Indictment's conclusory assertion that they constitute a "material misrepresentation" suggests it will urge the jury to find them false or misleading in some way. But the Indictment says nothing about what information they allegedly conveyed or how that information was supposedly false or misleading. *See* p. 23, *supra*.

The same problems inure to the alleged "False Signature." The Indictment says next to nothing about the factual content of the False Signature other than that the Peraire-Buenos "knew that *the information*" in the signature "could not be verified for ultimate publication to the blockchain." Indict. ¶ 26 (emphasis added). The Indictment fails to identify that "information" or explain why it could not be verified. Instead, the Indictment jumps to the alleged *consequence* of the False Signature—*i.e.*, that it "trick[ed] the Relay to prematurely release the full content of the proposed block." *Id.* But this inadequate allegation only exacerbates the vagueness problem. As the Indictment recognizes, the relay was not a person but rather open-source computer code; indeed, it alleges elsewhere that the Peraire-Buenos "identifi[ed] and exploit[ed] a vulnerability in ***the MEV-Boost relay code*** that caused the relay to prematurely release the full content of the proposed block." *Id.* ¶ 17 (emphasis added). What does it even mean to trick the "relay code," if there is no allegation that the Peraire-Buenos gained unauthorized access to any computer system or altered any computer code? If the relay's publicly viewable code permitted its release of the contents of the proposed block, how could the relay have been tricked? The Indictment fails to answer these critical questions about the alleged fraud.

Elsewhere, the Indictment gestures vaguely at the idea that a validator's signature conveys some other meaning or commitment but it does not say precisely what or how. In its background allegations, the Indictment alleges that a relay "initially only submits the 'blockheader' to the validator, which contains information about . . . the payment a validator will receive for validating

the proposed block as structured by the builder." *Id.* ¶ 13 (emphasis omitted). That preview of the payment is a communication ***from the relay to the validator***. In the very next sentence, however, the Indictment pivots to say that "[i]t is only ***after the validator*** makes ***this commitment*** through a digital signature that the relay releases the full content of the proposed block . . . to the validator." *Id.* (emphases added).[22] What is that alleged "commitment," where does it come from, and to whom is it directed? Does the commitment come in the form of the signature itself or through some other agreement? If the latter, what agreement? The Indictment does not allege that, by becoming validators, the Peraire-Buenos agreed to validate the block as structured by the builder (and sent by the relay) or were under any duty to do so. And the while the Indictment appears to allege that the Peraire-Buenos violated the expectations of some other users on a decentralized cryptocurrency exchange, it does not identify where those norms purportedly governing participants' behavior can be found.

Finally, the Indictment's theory of property loss is fatally unclear. While the Indictment alleges at times that the Peraire-Buenos "stole" the alleged victims' cryptocurrencies, Indict. ¶ 1, its allegations regarding the transactions at issue contradict that conclusory assertion by alleging that their MEV Bots traded away the cryptocurrencies in their frontrun trades. *See* pp. 8-9, *supra*. The Indictment does not allege the MEV Bots retained any rights to those currencies, leaving undefined the nature of the supposedly impaired property rights at issue.

Accordingly, the Indictment's theory of falsity regarding the alleged Lure Transactions and False Signature, and its theory of property loss is intolerably unclear.[23] *See United States v. Curtis*,

---

[22] *See also id.* ¶ 14 (alleging that the relay will not release the block "until the validator has confirmed through a digital signature that it will publish the proposed block as structured by the builder to the blockchain").

[23] The Peraire-Buenos have sought this information from the government to no avail. In a September 26, 2024 letter, the Peraire-Buenos requested "[e]ach statement or representation

506 F.2d 985, 992 (10th Cir. 1974) (dismissing vague mail fraud indictment and noting that simply labeling "acts, documents or conduct innocuous in themselves" false "did more to confuse that to clarify"). The lack of specificity poses two related problems. First, the Peraire-Buenos have not been adequately informed of the nature of the accusations against them, as is their right under the Sixth Amendment. *Walsh*, 194 F.3d at 44. They cannot adequately prepare to defend against the allegations when the Indictment's framing of the alleged fraud is so muddled. Second, the government's unclear theories could allow the prosecution to deviate from the facts and theories presented to the grand jury, in violation of the Fifth Amendment. *Id.* The Indictment leaves the government free to amend its theory of falsity up to, and even during, trial. It must be dismissed.

IV. THE MONEY LAUNDERING COUNT ALSO MUST BE DISMISSED.

For the reasons discussed above, the Court should dismiss Counts One and Two of the Indictment for (a) lack of fair notice that the alleged conduct could be considered criminal; (b) failure to sufficiently allege the essential elements; (c) failure to allege sufficient facts going to the core of the alleged fraud. Dismissal of the fraud charges on any of these grounds requires dismissal of the money laundering charges predicated on the proceeds of that alleged fraud. *See United States v. D'Alessio*, 822 F. Supp. 1134, 1146 (D.N.J. 1993) (where "mail fraud" charges are dismissed, a money laundering charge dependent on that same mail fraud must also be dismissed).

CONCLUSION

For the reasons set forth above, the Court should dismiss the Indictment.

---

alleged to be false or misleading, to whom the government contends it was made, and a description as to how it is allegedly false or misleading." Declaration of Katherine Trefz, Ex. 3 at 1. The government declined to provide the requested particulars. In any event, "it is a settled rule that a bill of particulars cannot save an invalid indictment." *Russell*, 369 U.S. at 770.

Date: December 6, 2024

Respectfully submitted,

By: */s/ Katherine Trefz*

Katherine Trefz (*pro hac vice*)
Daniel Shanahan (*pro hac vice*)
Patrick J. Looby (*pro hac vice pending*)
Williams & Connolly LLP
680 Maine Avenue SW
Washington, DC 20024
Tel: (202) 434-5000
ktrefz@wc.com
dshanahan@wc.com

Jonathan P. Bach
Shapiro Arato Bach
1140 Avenue of the Americas
17th Floor
New York, NY 10036
Tel: 212-257-4897
jbach@shapiroarato.com

Counsel for Defendant
James Peraire-Bueno

By: */s/ Daniel N. Marx*

Daniel N. Marx
William W. Fick (*pro hac vice*)
Fick & Marx LLP
24 Federal Street, 4th Floor
Boston, MA 02110
Tel: 857-321-8360
dmarx@fickmarx.com
wfick@fickmarx.com

Counsel for Defendant
Anton Peraire-Bueno

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2024, I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will send notification of such filing to all counsel of record in this matter who are on the CM/ECF system.

/s/ Katherine Trefz
Katherine Trefz